
دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

الجريمة والقرصنة في مجال المعلوماتية والشبكات

د . محمد زايد

1) المقدمة:

تعد القرصنة والتخريب في مجال المعلوماتية والشبكات من الجرائم الحديثة التي رصدت جهود وأموال طائلة للقضاء عليها والتصدي لها ومنعها من الانتشار، وذلك للضرر المادي الذي تسببه هذه الجرائم. وتنمو هذه الجرائم وتتعدد بالتوازي مع نمو تقانات المعلومات والاتصال، وتتكيف حسب الاتجاهات التي تسلكها هذه الأخيرة. وقد تنامت الأعمال الإجرامية والتخريبية نظرا إلى أنّ قطاع المعلوماتية والاتصال أصبح ركيزة أساسية لنمو الاقتصاد العالمي وعنصرا فعالا في وضع إستراتيجياته ومشاريعه المستقبلية. وقد تكاثر المخربون والقراصنة عندما ظهرت شبكة الإنترنت وازداد تطورها وأصبحت ركيزة أساسية للاقتصاد العالمي المادي واللامادي، حيث وجد هؤلاء أرضية خصبة للتأثير، خاصة أنّ جلّ الأعمال التخريبية والقرصنة تتم على الشبكة العالمية والحواسيب المرتبطة بها سواء كانت موزعات أو خادمات أو حواسيب عادية تعمل كمطاريف أو حواسيب مرتبطة بشبكات محلية ترتبط بدورها بشبكات أخرى إلى أن غطت العالم كله. وقد تعددت طرق التخريب ومنها القرصنة بهدف سياسي أو بهدف شخصي (نجد ذلك عند الشباب المخرب الذي يتبارى مع الآخر في إمكانية النفاذ إلى الحواسيب أو المواقع أو المنظومات المعلوماتية المحصنة أو المحمية نظرا لأهمية المعطيات المخزنة فيها أو البرمجيات الباهظة الثمن أو لأسرار أخرى وضعت في ملفات سرية) أو لمجرد تلبية دافع داخلي. وقد أصبحت الأعمال التخريبية والإجرامية ظاهرة عالمية حقيقية تهدد المصالح الحيوية والاقتصادية للأشخاص والمؤسسات والدول.

وفي هذا السياق نتناول موضوع الجريمة في المعلوماتية والشبكات فنتعرف على مفهومها، وعلى مختلف طرقها والآليات المستعملة فيها، ثم طرق التعامل معها والتصدي لها، وأخيرا وسائل الحماية والسلامة لمنعها والحد من انتشارها، ونختم دراستنا بالبحوث الجارية لتطوير طرق التصدي والحماية.

2) مفهوم الجريمة في المعلوماتية والشبكات:

االجريمة المعلوماتية هي "السلوك السيء المتعمد الذي يستخدم نظم المعلومات لإتلاف المعطيات أو إساءة استخدامها مما يتسبب أو يحاول التسبب إما في إلحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها"[1]. والمجرم المعلوماتي هو إنسان قام بأعمال تخريبية أو إجرامية تتعلق بمجال المعلوماتية أو شبكات المعلوماتية. وقد ظهرت أسماء في ميدان الجريمة المعلوماتية لتصف مرتكبيها، فمنهم "الهاكار[2]" و"الكراكر[3]". وتتمثل الجريمة المعلوماتية جريمة مجال والشبكات في النفاذ أو اختراق منظومة للوصول إلى معلومات محمية ومحصنة سواء كانت سرية أو شخصية وغير مرخص لأي شخص أن يطلع عليها أو يستعملها في أغراض شتى دون إذن من أصحاب هذه المعلومات أو المعطيات التي تكون غالبا في شكل ملفات معلوماتية مخزنة على حاسوب أو عدة حواسيب وتكون الحواسيب قريبة من بعضها بعضا أو متباعدة. ويصل الإجرام إلى إتلاف تلك المعلومات أو تعطيل الحواسيب المركزة عليها بهدف الإضرار بأصحابها سواء كانوا أفرادا أو مؤسسات أو حكومات أو غيرها. وتصنف العمليات الإجرامية في مجال المعلوماتية والشبكات إلى عدة أصناف منها الاختراق والابتزاز وفك التشفير السري وامتصاص المعلومات عبر أجهزة جاسوسية تقوم بالتقاط تلك المعلومات ومعالجتها للاستفادة منها، وهناك أصناف أخرى من الأعمال الإجرامية التي تعتمد المعطيات المخزنة على الحواسيب لأغراض تتعلق بالسطو المالي على ممتلكات الأفراد والمؤسسات من الأموال والمنتجات عبر قرصنة أرقام الحسابات البنكية. ويتلخص الإجرام المعلوماتي والشبكي في قسمين أساسيين هما التخريب والقرصنة.

---

1 المجلة العربية للعلوم والمعلومات: العدد 3، يونيو 2004: الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات في التشريع السوري والتشاريع المقارنة، ص 113.

Hacker 2

Cracker 3

– التخريب: هي عملية اختراق أو نفاذ غير مرخص لصاحبها، يقوم خلالها بإتلاف المعطيات والمعلومات وكل ما يعتبر عنصرا أساسيا في تشغيل المنظومة المعلوماتية أو الشبكية المعنية كفسخ محتوى لاحقات التخزين كالأقراص الصلبة وأجهزة التخزين الأخرى أو إدخال برمجيات غريبة عن المنظومة تقوم بتعطيل المنظومة وتمنع صاحبها الحقيقي من استعمالها واستغلالها أو حتى النفاذ إليها أو تشغيلها.

– القرصنة: هي عملية اختراق لمنظومات حاسوبية أو شبكية يتم خلالها نسخ المعلومات المراد قرصنتها بهدف استغلالها لأغراض شخصية سواء منها الربح المالي أو لأغراض أخرى كالتشهير أو التجسس الصناعي أو التجسس الأمني أو التحيل أو غير ذلك من الأعمال الإجرامية المشابهة والواقعة في الحياة اليومية في المجالات المختلفة كالتزوير والسرقة والتنصت وغير ذلك. ويمكن تصنيف القراصنة إلى عدة أصناف منها:

– القراصنة الذين يعملون على فك شفرات البرمجيات المحمية لاستعمالها ويسمون "الكراكر".

– القراصنة الذين يعمدون إلى فك شفرات البطاقات بكل أصنافها سواء كانت بنكية أو غيرها ويسمى هذا الصنف "الكاردر[4]".

– القراصنة الذين يعمدون إلى فك شفرات منظومات الهاتف السلكي ويسمى هذا الصنف "الفريكر[5]".

كما تم تصنيف القراصنة إلى مجموعات أخرى حسب الاتجاهات والأهداف وأسندت إليها أسماء قبعات وهي على التوالي:

– القبعات البيضاء[6]: وهي المجموعات ذات المصلحة من المنظومات المعلوماتية كالمستشارين في المعلوماتية ومديري الشبكات والشرطة المعلوماتية. ويقوم أفراد هذه المجموعة باختبارات في الاختراقات بالاتفاق مع أصحاب المنظومات لتحسين جودة الحماية لهذه المنظومات. ويمكن لهؤلاء أن يكونوا باحثين في اكتشاف نواقص برمجيات الحماية وتحليل المنظومات التشغيلية والبروتوكولات بهدف إدخال تحسينات في الحلول الوقائية ضد تهديدات القراصنة الآخرين.

Carder 4

Phreaker 5

Hackers Hat White 6

- القبعات السوداء[7]: وهي مجموعة تقوم بإنجاز الفيروسات والبرمجيات الجاسوسية والتخريبية.
- اللصوص: وهي من المجموعات المؤذية التي تدفعها عدة أغراض عكس القبعات البيضاء.

ونجد داخل المجموعة عدة أصناف أخرى من القراصنة منهم "الهاكتيفيست[8]" الذين يقومون بالأعمال التخريبية لأغراض إشهارية ولأسباب إيديولوجية، ومنهم "الكراشور[9]" الذين يدمرون المنظومات والبرمجيات المعلوماتية بدون عدوانية لأصحابها ولكن حبا في تلك الأعمال.

- القبعات البنية[10]: وهي المجموعات التي تقع بين القبعات البيضاء والقبعات السوداء والتي تتسلل إلى المنظومات والشبكات المعلوماتية دون إلحاق الضرر بها أو إيذائها أو بهدف التدمير أو القرصنة.

3) طرق التخريب والقرصنة وآلياتها:

تتمثل عملية القرصنة والتخريب أولا في كيفية الاختراق أو التسلل أو النفاذ خلسة إلى المواقع المعلوماتية والشبكية المقصودة من هذه الأعمال ثم في الأعمال الممكن القيام بها عند الوصول إلى الهدف. وفي هذا السياق تتعدد طرق وأساليب القرصنة والتخريب في مجال المعلوماتية والشبكات حسب الأهداف والأغراض التي يرمي إليها فاعلوها. ويمكن أن نقسمها إلى ثلاث طرق أساسية هي:

أ- طرق وأساليب لسرقة المعطيات والمعلومات وذلك بالتسلل إلى المواقع التي خزنت عليها هذه المعطيات.

وتجرى غالبية هذه الأعمال على الشبكات المعلوماتية بإرسال برمجيات إلى الجهاز الهدف، وتكون تلك البرمجيات في شكل رسائل أو في شكل برمجية سرية تتسلل إلى الجهاز وتلتقط المعلومات ثم ترسلها إلى الجهاز المخرب. وعادة ما تتم هذه العملية على شبكة الإنترنت باستعمال البريد الإلكتروني الذي يحتوي على عناوين شخصية لأصحاب الأجهزة والمنظومات المعرضة للقرصنة والتخريب. ويمكن أن تكون البرمجيات المضرة متمثلة في برمجيات جاسوسية تلتقط العناوين أو برمجيات نسخ وتشفير وهي برمجيات

Hackers Hat Black 7
Hacktivistes 8
Crashers 9
Hackers Hat Grey 10

تنصت وجوسسة. وتعتمد هذه الأعمال أساسا على فك التشفير لآليات السلامة والحماية، وهو كسر المفاتيح السرية وكلمات السر التي تمنع غير المرخص لهم من النفاذ واستعمال المنظومات.

ب- طرق وأساليب لتدمير المعطيات وتعطيل المنظومات، ويتمثل ذلك في إرسال برمجيات مضرة وتعرف بالفيروسات والديدان التي تعد اليوم من أخطر الطرق المدمرة والمضرة بالمنظومات المعلوماتية والشبكية. وتتمثل الطريقة في بث رسائل بريدية إلى الأجهزة والمنظومات المراد إيذاؤها، وعند فتح تلك الرسائل تثبت البرمجية الخبيثة على الحاسوب وتشرع في نشاطها المخرب سواء بإجراء عمليات كتابة على البرمجيات الأساسية للمنظومات التشغيلية لتعطيلها تماما أو القيام بعمليات نسخ لمعطيات لا علاقة لها بالمنظومة وتثبيتها في المساحات المعدة لتخزين المعطيات كالذاكرات أو الأقراص الصلبة إلى غاية امتلاء تلك الفضاءات وعجز الحاسوب أو الشبكة على الاشتغال.

ت- طرق وأساليب لتحويل مبالغ مالية أو تغيير مسار منظومات معلوماتية لأغراض مضرة بالمجتمع أو بمؤسسة أو شخص ما أو المساومة. ويتمثل ذلك في النفاذ إلى الموزعات التي تحتوي على شفرات البطاقات البنكية التابعة لحرفاء البنك أو المؤسسة المالية التي تم اختراق حواسيبها ومنظوماتها المعلوماتية، كما يتم تحويل المبالغ المالية من حساب إلى آخر بأمر برمجياتي كما هو في الحالات العادية في المبادلات المالية والصفقات التجارية أو تحويل وجهات البضائع والمنتوجات من مكان المعد للاستلام الصحيح إلى مكان آخر يتلقاها اللص أو مجموعة اللصوص الذين قاموا بالعملية بواسطة الأنظمة الحاسوبية وغير ذلك من الأعمال المخربة والإجرامية.

أما الآليات والتقنيات المعتمدة فهي الآتية:

- البرمجيات الهجومية: وهي البرمجيات المنجزة بغرض الضرر بالمنظومات المعلوماتية والشبكية وتعطيلها. ونذكر منها:

* الفيروسات[11]: وهي برمجيات تقوم باستنساخ نفسها على الحواسيب التي تنفذ إليها.

Virus 11

* الديدان[12]: وهي برمجيات تقوم بالتعرف على الموارد البرمجية في الحاسوب والعمل على استنساخ تلك الموارد.

* حصان طروادة[13]: وهي في الظاهر برمجيات عادية لكنها تقوم بتفعيل برمجيات جزئية غير مرخص لها على الحاسوب.

* الباب الخلفي[14]: وهي برمجية تقوم بفتح منفذ غير مرخص على منظومة معلوماتية غالبا ما تكون عن بعد عبر الشبكات المرتبطة بذلك الحاسوب.

* البرمجية الجاسوس[15]: وهي عبارة عن برمجيات تقوم بجمع معلومات خاصة بالمستعمل وإرسالها إلى الشخص أو الأشخاص المعنيين بهذه القرصنة.

* مسجل المفاتيح[16]: وهي برمجية تقوم بالتسجيل كلما تم الضغط على مفتاح من مفاتيح اللوحة، وعادة ما تكون هذه البرمجية مركزة على حاسوب المستعمل دون إيقاظه بذلك.

* المستغل[17]: وهو عبارة عن برمجية تقوم باستغلال العيب في منظومة الحماية والسلامة لإلحاق الضرر بها وبالحاسوب والشبكة التي ركزت عليها هذه المنظومة.

* برمجية عدة الجذور[18]: وهي برمجيات تقوم بالتقاط كل المفاتيح وكلمات السر وتنسب للمخترق كل الصلوحيات لإدارة الحاسوب أو الشبكة المخترقة مع فتح منفذ خلفي وفسخ كل آثار الاختراق.

– تقنيات الهجوم عبر البريد الإلكتروني:

علاوة على البرمجيات الهجومية التي تكتسح البريد الإلكتروني، هناك هجمات خاصة تقوم بها برمجيات منجزة للغرض وهي:

* الرسائل الإشهارية أو التافهة[19]: وهي رسائل تافهة تقوم بزحم قنوات الوصل بين الشبكات وتضيع الوقت لمستقبلي تلك الرسائل.

* الرسائل الصائدة[20]: وهي رسائل توجه باسم مؤسسات مالية أو شركات تجارية تطلب من صاحب الحاسوب أو المنظومة المعلوماتية معلومات سرية يتم استغلالها من طرف صاحب الرسائل.

---

12 Worm
13 Trojan
14 Backdoor
15 Spyware
16 Keylogger
17 Exploit
18 Rootkit
19 Spam
20 Phishing

* الطرفة أو النكتة المعلوماتية[21]: وهي عبارة عن رسالة تبث على الشبكات والمنظومات المعلوماتية تدعو المستعملين إلى إعادة توجيه تلك الرسائل إلى أصدقائهم، وذلك لزحم قنوات الاتصال في الشبكات ولإضاعة وقت المستعملين. ويطلب في بعض الأحيان من المستعملين القيام بأعمال تخرب البرمجيات كفسخ ملفات تابعة لمنظومة التشغيل بدعوى أن تلك الملفات تحتوي على فيروسات.

- الهجوم على الشبكات المعلوماتية:

ومن الطرق الشائعة في تخريب قواعد البيانات الضخمة المركزة على الحواسيب المرتبطة بالأنترنت عملية التصنت والتجسس المعروفة وذلك بواسطة برمجية ترسل على الشبكة لتتبع دفق المعلومات المتبادلة بين الحواسيب والتقاطها مع نسخها على حاسوب القراصنة. وبواسطة هذه الطريقة يمكن القيام بالأعمال الأخرى المضرة والمخربة بالمنظومات المعلوماتية والشبكات.

4) وسائل التصدي والحماية:

نظرا لخطورة أعمال التخريب وللضرر اللاحق بمنظومات المعلومات والحواسيب والشبكات وبالتالي للاقتصاد العالمي بسبب هذه الجرائم المعلوماتية والشبكية (حيث أن الإحصائيات الأخيرة تؤكد أن قطاع تقانات المعلومات هو المحرك الأساسي للاقتصاد العالمي ويساهم ب 180 مليار دولار من الضرائب سنويا ويشغل 9 ملايين شخص وإن كان معدل القرصنة في العالم بلغ 35 في المائة سنة 2004)، فإنّه للحد من ذلك وضع المختصون عدة أساليب وطرق تكون في الغالب متكاملة وهي كالتالي:

- البرمجيات المضادة للفيروسات والديدان، وهي برمجيات صممت وأنجزت للتعرف على الفيروس أو الدودة وإبطال مفعولها بتجميدها إن لم تستطع حذفها ومسحها من على الجهاز أو المنظومة. وقد اختصت عدة شركات في تصميم وإنجاز تلك البرمجيات المضادة، لكن القراصنة والمخربين لا يكفون عن تطوير منتجاتهم مما يجعل شركات الحماية والسلامة مضطرة إلى تحديث منتجاتها كي تحد من مفعول البرمجيات الخبيثة. وقد توصّل منتجو البرمجيات المضادة إلى تصميم برمجيات أخرى تتكامل مع البرمجيات المضادة لمكافحة الفيروسات والديدان وكل البرمجيات المضرة الأخرى.

- برمجيات التحري والتقصي لرصد التحركات والسلوكيات المريبة للبرمجيات داخل

Hoax 21

الحواسيب والمنظومات. وعندما يتبين ذلك يتمّ إيقاف تلك البرمجيات واستخدام محرك مسح البرمجيات الفيروسية التي تقوم بالقضاء على تهديداتها قبل أن تشرع في الاشتغال.

- برمجيات الوقاية والسلامة المسماة بجدران النار، وهي منظومات تتمثل في أجهزة مختصة في تقصي البرمجيات المضرة والمخربة أو الجاسوسة. وتركز هذه المنظومات سواء على حواسيب منفردة أو على شبكات. وتعمل هذه المنظومات على مراقبة كل المعطيات النافذة وتقوم بتحليلها حسب المعلومات والأوامر التي تلقتها في شكل ملفات وعناصر تركز عليها ومنها العناوين التي يمكن السماح لها بالنفاذ والعناوين غير المرخص لها و التثبت في كل ما يتصل بالعناوين من كلمات سر ومفاتيح سرية أخرى والبيانات التي تتصل بحقوق النفاذ إلى المعلومات التي وضعها مدير المنظومة لمستعمليها. ويمكن تركيز جملة من البرمجيات الوقائية داخل هذه المنظومة للتصدي إلى الهجومات الإجرامية قبل أن تنفذ إلى المنظومات المعلوماتية وقواعد البيانات.

- برمجيات مراقبة النفاذ، وهي برمجيات غالبا ما تكون جزءا من أجزاء منظومات التشغيل على الحواسيب الفردية أو شبكات الحواسيب. وتقوم هذه البرمجيات بمراقبة مستعملي المنظومة ومقارنة مفاتيح السر التي يدخلها المستعمل على المنظومة بما هو مركز على تلك المنظومة. كما أنّ لهذه البرمجيات صلوحية منع المستعملين الذين لا يدلون بهوية صحيحة ومطابقة للبيانات المركزة على المنظومة، مما يحد من عملية التسلل أو الاختراق للقراصنة المبتدئين. وقد عمل منتجو منظومات التشغيل على إضافة عدة آليات حماية وصلت إلى إخفاء السجلات الحساسة أو تشفيرها مما يصعب على غير المرخص لهم من مستعملي المنظومات استغلال المعلومات أو حتى الاطلاع عليها.وأصبح موضوع الحماية والسلامة في المنظومات عنصرا أساسيا في التنافس لكسب السوق العالمي.

5) **السلامة والحماية:**

أصبح موضوع الأمن والسلامة الهاجس الكبير في قطاع تكنولوجيا المعلومات، مما دفع جل المهتمين بهذا القطاع إلى تكثيف الجهود ووضع آليات مختلفة للتصدي للجريمة المعلوماتية، فشرّعت الدول القوانين لمعاقبة المجرمين، واخترعت المؤسسات العلمية والصناعية طرقا

وآليات متطورة إضافة إلى ما تمّ تحديثه من طرق وآليات قديمة.

أما على الصعيد التقاني والطرق المستحدثة فقد وجد المهتمون بموضوع السلامة والحماية في التقنية البيومترية[22] حلا مناسبا ومقنعا للتأمين والوقاية سواء في المنظومات المعلوماتية أو القطاعات الأخرى التي تستدعي التثبت والتأكد من هوية المستعمل. كما تستعمل هذه التقنية من جهة أخرى لكشف المجرمين ومعاقبتهم، فهي تقنية وقائية وردعية.

وتتمثل التقنية البيومترية في عدة تقنيات ثانوية هي:

* التعرف على بصمات الأصابع والأيدي البشرية ومعالجتها بواسطة المعلوماتية، حيث يتم إدخال بصمة أو بصمات المستعملين على قاعدة بيانات المنظومة المراد حمايتها ثم يتم بعد ذلك مقارنة المستعملين بالبصمات المخزنة داخل القاعدة. وتستطيع تقنية التعرف على البصمات مع الآليات الأخرى أن تحمي المنظومة المعلوماتية أو الشبكات من الاختراق وتمنع القراصنة من القيام بأعمال الاختلاس أو السرقة، ويتم ذلك في الموزعات البنكية أو مخابر أو مراكز بحث مهمة وغير ذلك.

* التعرف على قرنية العين، وهي تقنية حديثة تتمثل في إدخال قرنية العين إلى منظومة معلوماتية عبر كاميرا رقمية، ويتم تحليل خصائص تلك القرنية وتخزينها على قاعدة بيانات يتم تحليلها ومقارنتها بقرنيات المستعملين الآخرين، وبذلك يمكن التصدي لكل غريب يريد النفاذ إلى المنظومة أو الشبكة. وغالبا ما يتم اعتماد هذه التقنية مع تقنية التعرف على البصمات في الموزعات البنكية وعند النفاذ إلى مراكز أو مخابر أو أماكن غير مرخص للنفاذ إليها.

* التعرف على الإمضاء الإلكتروني، وهي تقنية قديمة نسبيًّا لكنه تم الاهتمام بها أكثر عندما تقدمت البحوث في التعرف على الأشكال، فأصبحت هذه التقنية تضاهي في أهميتها التقنيات البيومترية السالف ذكرها. ويتمثل استعمال تقنية التعرف على الإمضاء في إدخال الإمضاء الفعلي للمستعمل، ويتم تحليل ذلك من طرف المنظومة وتخزينها على قاعدة بيانات وتصبح مرجعا عند كل عملية نفاذ حيث يتم مقارنة الإمضاء الحالي بجملة الإمضاءات المخزنة في المنظومة للسماح بالنفاذ والقيام بالأعمال أو منع المستعمل من ذلك.

Biometry 22

* وهناك تقنيات أخرى بيومترية كالتعرف وتحليل الجينات البشرية وعلى الأوعية الدموية للإنسان والتي غالبا ما تطبق في ميدان مكافحة الجريمة بكل أنواعها.

أما على الصعيد التشريعي والقانوني فإنّ جل دول العالم قد وضعت قوانين تتعلق بالجريمة في مجال المعلوماتية والشبكات، وقد توصلت بعض الكتل الإقليمية إلى توحيد قوانينها وسن قوانين موحدة في هذا المجال نذكر منها أروبا والولايات المتحدة وغيرها من الدول التي تعتمد في اقتصادها أكثر فأكثر على قطاع تقانات المعلومات. ونقدم فيما يلي مثالا من التشريع البلجيكي لمحاربة الجريمة في المعلوماتية وفي تقانات المعلومات:

قسم المشرع البلجيكي[23] الجرائم المعلوماتية إلى أربعة أقسام تندرج تحت جريمة "التزوير واستعمال المزور" (الفصل 210 & 1) وينص القانون على معاقبة "كل إنسان يرتكب التزوير بإدخاله في منظومة معلوماتية لتغيير أو فسخ معطيات مخزنة معالجة أو مرسلة من طرف منظومة معلوماتية أو تغيير بواسطة أي طريقة إلكترونية في استعمال ممكن للمعطيات داخل منظومة معلوماتية وبذلك بهدف التغيير الشرعي للمعطيات."

وتنقسم الجريمة إلى أربعة أقسام :

ـ التدليس واستعمال التزوير :

إنجاز العقود الإلكترونية المزورة أو استعمال بطاقات بنكية للقروض أو التسديد المالي مزورة يمثل نماذج للتزوير المعلوماتي. وخلافا للتدليس في الكتابات العادية أي في القانون المدني،فإن التزوير في المعلوماتية لا يلفت الانتباه.فعملية التزوير في المعلوماتية أو محاولة استعماله يعاقب صاحبها بالسجن لمدة تتراوح بين ست وخمس سنوات وبغرامة مالية تتراوح بين 26 و100000 فرنك.

ـ الاحتيال ومحاولة استعمال الغش :

عملية الاحتيال في المعلوماتية أو محاولة استعماله يعد من أعمال التزوير في المعلوماتية. وهذا الإجراء يجعل الشخص المحتال هو الذي يتحصل على وثائق معلوماتية لنفسه أو لغيره بواسطة الغش قصدا أو عن غير قصد للانتفاع سواء بإدخال أو تغيير أو فسخ معطيات مخزنة أو معالجة أو مرسلة في منظومة معلوماتية. ومن بين الأعمال التي تقع تحت طائلة القانون:

– استعمال بطاقة بنكية للقروض أو للتسديد المالي مسروقة.

---

23 http://www.awt.be/web/fic/index.aspx?page=fic,fr,j00,014,003

- إدخال أوامر برمجية بهدف اختلاس أموال.

- تغيير وجهة برمجيات أو ملفات بهدف الاستفادة المادية.

أما العقوبات المتعلقة بهذه الأعمال فهي نفسها المقررة لعملية التدليس ومحاولة استعمال الغش في المعلوماتية .لكنه تم تخصيص عقوبات أكثر صرامة للأشخاص الذين يعيدون ارتكاب نفس الجريمة.

- الاختراق والنفاذ غير المرخص فيه:

تعرّف عملية الاختراق في التشريع البلجيكي بأنها النفاذ غير المرخص فيه إلى المعطيات أو منظومة معلوماتية أو جانب منها والمكوث فيها. وتتمثل عقوبة عملية الاختراق أو محاولته في السجن لمدة تتراوح من 3 أشهر إلى سنة مع/أو غرامة مالية تتراوح بين 26 و25000 فرنك. ويهدف نص القانون إلى منع محاولات الاختراق الخارجية والداخلية التي تتمثل عقوباتها في السجن من 6 أشهر إلى سنتين، وذلك لأن العملية الداخلية تهدف إلى الضرر. ويهدف الاختراق سواء في الاطلاع أو اختلاس معطيات للفاعل أو لغيره. ويتعرض صاحب الأمر في الاختلاس إلى عقوبة سجن تصل إلى خمس سنوات و/أو غرامة مالية بـ 200000 فرنك. ويمثل استعمال تقنيات لإلحاق الضرر بمنظومات معلوماتية أعمالا خطيرة. أما المساومة والتجارة بهذه المعطيات فتمثل أعمالا خطيرة يعاقب عليها خاصة عند تكرارها.

وقد سن المشرع البلجيكي أحكاما تدريجية تتماشى مع نسبة الأضرار الحاصلة التي هي كالتالي:

- تخريب المعطيات
- تخريب للمعطيات تنتج عنه أضرار
- تخريب منظومة معلوماتية
- كل الاستعمالات ذات قصد احتيالي ينجم عنها تخريب. ويعني ذلك النظرية الأخيرة التي تهدف إلى بث الفيروسات المعلوماتية.

6) الخاتمـة:

تعد محاربة الجريمة المعلوماتية أمرا مفروضا على كل دول العالم وخاصة منها التي تعتمد على قطاع تقانات المعلومات كركيزة أساسية لنمو اقتصادها. وحسب الإحصائيات والدراسات الأخيرة فإن الجريمة المعلوماتية قد ألحقت ضررا فادحا وخسارة مالية تقدر ب23 مليار دولار، حيث وصلت نسبة القرصنة في بعض الدول إلى 75 بالمائة بل 90 بالمائة في دول أخرى العام الماضي (2005).

وقد ترجع أسباب القرصنة أساسا إلى أنّ بعض الشركات والمؤسسات قد استحوذت على قطاع

تقانات المعلومات وجعلته فضاء مغلقا مما أدى إلى بروز مجموعات مختصة في المجال تعارض فكرة الهيمنة، فشرعت في مقاومة هذا السلوك التجاري وكانت أساليب المقاومة نوعين: نوع في ظل القانون وذلك بإنجاز منتجات مضادة ومفتوحة تنافس منتجات الشركات المهيمنة كمنظومات الاشتغال. فقد تم إنجاز منظومة تشغيل لونيكس من طرف باحثين جامعيين لمنافسة شرعية لمنظومة ويندوز المهيمنة. وقد أدى ذلك إلى ظهور تيار كبير من المختصين في المجال لمساعدة المنظومة المفتوحة، وظهرت صناعة البرمجيات في هذا الإطار وسمّيت بالبرمجيات مفتوحة المصدر وأصبحت تحتل مكانة كبيرة في مجال المنظومات المعلوماتية وتقانات المعلومات، مما أجبر الشركات العالمية المضادة على فتح برمجياتها ومنظوماتها لهذا الصنف من البرمجيات. لكن التيار المسالم في منافسة العالم الراسمالي قليل مقارنة المخرب بالتيّار الذي يعتمد الأساليب الإجرامية لمحاربة المنتجات الرأسمالية. وقد وجد المخربون والمجرمون فضاء للنشاط فاختلط ذوو المبادئ بالمجرمين والقراصنة واعتمدوا طرقا إجرامية لأهداف مختلفة، لكن النتيجة واحدة وهي تدمير وإتلاف المعلومات وتعطيل المنظومات المعلوماتية والشبكات التي تعتبر البنية الأساسية لتقانات المعلومات ومجتمع المعرفة.

ورغم الجرائم المرتكبة والتخريب، فإن هذه الأعمال تدفع المهتمين بمجال تقانات المعلوماتية والشبكات إلى مزيد البحث لتطوير القطاع والوصول إلى حلول وقائية وحماية أكثر فاعلية ونجاعة. ومن جهة أخرى أصبحت الشركات المعنية تستقطب القراصنة والمجرمين للاستفادة من خبراتهم ومهاراتهم مما يجعل القطاع. ينتفع من جانبين: الجانب الأول هو نقل المجرم واللص من صف المجرمين إلى صف المصلحين والعاملين والمساهمين في تنمية القطاع وعادة ما يقوم هؤلاء الإفراد باختبار منظومات الوقاية والحماية لمنظومات المؤسسات وشبكاتها كما يقومون بكشف التسللات والاختراقات التي يقوم بها زملاؤهم .لكن ليت كل المجرمين يصبحون مصلحين!! فالحرب قائمة لأن المنافع كبيرة وكثيرة ومغرية.